General Services Administration
Mid-Atlantic Region

Performance Work Statement (PWS)
for
Project Manager Mission Command (PM MC)
Mission Command Support Center (MCSC)

1.0 BACKGROUND.

Project Manager Mission Command (PM MC) provides leaders and Soldiers with the mission command and situational awareness capabilities that have fundamentally changed American warfare, drastically improving our capability to execute full spectrum operations. PM MC products include computer hardware, software, communications and network management infrastructure to form an integrated system. Mission Command (MC) will be the principal command and control system for the Army and Marine Corps and provides users access to the tactical information necessary to achieve information dominance over the enemy. The Mission Command Support Center (MCSC) environment is in constant flux. New systems are added as they are developed and legacy systems are removed as they reach End of Life. As new mission requirements are added, the Government will provide guidance on how to incorporate these based on operational needs and requirements.

2.0 SCOPE.

This PWS covers all activities required to manage, operate, support, maintain, and sustain US Government Operations Centers located at Aberdeen Proving Ground, MD, Fort Carson, CO and Fort Hood, TX manage and operate multiple networks/domains, and sustain US Government assets located at multiple locations throughout the world. The following comprise the essential elements expected to be provided: Operations Management, Systems Operation and Sustainment, Technology Insertion, Installation/De-installation of Hardware (HW)/Software (SW), Satellite Network Operations, Internet Protocol (IP) Network Operations, Tier 1/2/3 Helpdesk, Training, Testing and Participation/Travel in Test Events, Active Directory administration, Information Assurance, Security, and any other functions directly pertaining to the MCSC. Any operational task that monitors or supports Command Control Communication Computer Intelligence Surveillance Reconnaissance (C4ISR) networks and systems within the purview of the Program Executive Office - Command, Control, & Communications-Tactical (PEO-C3T) falls within the scope of this PWS.

To account for the possibility that the Government's requirements may increase at a faster rate than currently projected, the Government reserves the right to increase the estimated overall ceiling value of this Task Order by as much as 25% per year of the Task Order (TO), if necessary. Such increases shall only apply to additional effort that clearly falls within the scope of the Performance Work Statement and within the performance period of the TO, including all available option periods.

Fluctuations in the Government’s requirements over the life of the TO are difficult to project at this time given uncertainties with the PM MC organizational structure and how it may impact the Information Technology (IT) services required in support of this task order. If support is required, the Government will specify the scope, timeline, and extent of such requirements post-award.

It is expected that Contractor will scale support (expands or contract resources) to provide appropriate staffing levels to meet the Government's emerging needs. The ceiling value of the task order will be adjusted to accommodate the potential increases or decreases associated with such change.

3.0 TASK ORDER REQUIREMENTS

NOTE: All labor will be awarded on a Firm Fixed Price (FFP) basis with the exception of 3.10 Government Directed Overtime/Surge, which will be awarded on a Labor Hour (LH) basis.

This is a performance-based effort. In order to increase the Government's confidence in the contractor's ability to achieve success, the following personnel positions and associated qualifications have been identified. The contractor shall meet the minimum qualifications for each position described within the timeframe indicated. Meeting these qualifications is a necessary, but not sufficient basis for contract success. All Information Technology/Cyber Security and Engineering support personnel shall meet the **DoD Approved 8570 Baseline Certifications for IAT II** (https://iase.disa.mil/iawip/Pages/iabaseline.aspx) and the performance standards (Identified in Performance Requirements Summary- PWS section 6.1.2) to be fully successful.

The contractor shall meet CMMI Level 3 for Services and CMMI Level 2 for Applications Development from the Prime contractor or from its Subcontractor or teaming partner.

Contractor personnel shall work Monday through Friday for 8 hours per day in accordance with the normal duty hours of the Government work locations for all PWS tasks **with the exception of PWS task 3.3 “Help Desk Support”**. On call support is necessary for all PWS tasks and may require contractor personnel to report to the Government work locations outside of their normal work hours.

PWS task 3.3 “Help Desk Support” requires on site contractor support 24 hours per day, 7 days per week and 365 days per year support including holidays and weekends. The contractor shall provide personnel to support three, (8) hour shifts per day to sustain this schedule at the Government work locations.

3.1 OPERATIONS MANAGEMENT SUPPORT

The contractor shall oversee and manage the overall operations of Government MCSCs. The operations management support duties shall include the following:

- Provide responses and reports (written & verbal) to the PM MC Project Manager and his/her designated representatives.
- Provide technical support to PM MC engineering personnel.

- Act as an interface between software development and test communities and the MCSC Operations Centers.
- Support PM MC with new IT technologies, development and integration.
- Serve as the Subject Matter Expert (SME) between the PM MC and PEO C3T Directorates in regards to Blue Force Tracking (BFT) operational sensitive matters.
- Create MC Operations Center supporting technical documentation.
- Review and edit technical documentation for content and accuracy.
- Attend meetings and provide technical briefings.
- Represent BFT Operations as a SME advisor of the Network Configuration Control Board.
- Engineer and implement new software to meet the requirements of PM MC.
- Provide 24 hours per day /7 days per week on-call support.

3.2 APPLICATIONS MANAGEMENT SUPPORT

The contractor shall manage software applications for the MC. Application management support to include the following:

- Interface with US and non-US Government agencies to provide or collect MC data, create special reports which shall require the gathering of required data from all MC Operations Center locations and outside sources.
- Conduct data management and data mining functions to create specialized daily, weekly and
- monthly reports.
- Develop software applications in coordination with PM MC or his/her designated representative(s).
- Provide ongoing support for the US Army MC/BFT program.
- Serve as a liaison between both Government personnel on-site and contractor support staff to address issues and provide feedback.
- Provide support to the development project team.
- Provide timely and periodic performance feedback/ input to the Project Manager.
- Responsible for the design, development and deployment of a scalable database driven web informational and customer service ticketing application(s).
- Provide full life cycle development of web pages and applications.
- Modify and build on existing applications.
- Employ leading edge technologies such as HTML, AJAX, JavaScript, PHP, SQL, APACHE, Flash, and Java in a Windows environment.
- Provide solutions to application change requests.
- Provide source code maintenance.
- Provide global database maintenance as it pertains to web based applications.
- Monitor website and database performance.
- Coordinate all mandatory maintenance activities, including hardware and software upgrades.
- Prepare and maintain project schedule, functional requirements, daily logs, and technical documentation.
- Create and provide training on new and existing applications, processes and procedures.

- Proactively provide ideas and solutions towards the improvement of the websites and applications.
- Ensure quality of deliverables through development and implementation of QA procedures and Standards.
- Provide technical support to the MC customer relations management system (CMR).
- Provide technical support to the Active Directory MC Network Essential X-Domain Unified System (NEXUS)
- Provide configuration and sustainment management for all software used within the BFT MCSC.
- Provide technical support to the MCSC helpdesk.

3.2.1 DATA ARCHITECTURE SUPPORT

The contractor shall manage the data architecture of the MC environment to include the following:

- Engineer, design and build relational databases for storing data from approved data sources.
- Architect data storage models and implement disaster recovery.
- Utilize advanced methodologies like data partitioning, multi-site data redundancy, multi-site data replication, off-site backups, and more industry standard policies.
- Eliminate single-points of failure.
- Ensure the safety of data structures with advanced archival and recovery solution.
- In addition to the software and products that shall be built and supported, architect strategies for all data-related tasks from database implementation, data storage, data policies, and archive/recovery. Routinely utilize updated requirements changes and store them in properly designed data storage models and continue to modify and update data schemas.
- Be familiar with the data format or Application Program Interfaces (APIs) of the following technologies:
    - Data Distribution Service (DDS)
    - Command and Control Registry (C2R)/ Command, Control, & Intelligence (C2I)
    - Data center environmental sensors
    - Lightweight Directory Access Protocol (LDAP)
    - Simple Network Management Protocol (SNMP)
    - Extensible Markup Language (XML)/ Extensible Markup Language Schema Definition Language
    - (XSD)/ Extensible Markup Language Style sheet Language for Transformations (XSLT)
- Manage and maintain advanced data warehouse environment.
- Create and maintain well-designed metadata repositories, detailed and indexed information about the structures that house the actual data.
- Interpret new and modified business needs and translate them into modern data architectures.
- Maintain normalized relational data structures, implement multi-dimensional databases, and Structured Query Language (SQL) when necessary.
- Implement alternative data storage models that are relevant and have real world benefits.
- Meet with team leads to discuss existing data warehousing setup and hardware.

- Meet with vendors / industry to ensure data storage hardware and software platforms are up to date with the latest advances.
- Upgrade data blueprints, object models, and entity-relationship models
- Work with vendors if needed to integrate third-party solutions.
- Conduct internal reviews of all data object designs, data models, and metadata structures.
- Meet to discuss improvements, upgrades to processes, procedures, and data management.

3.2.2 WEB DEVELOPMENT SUPPORT

The contractor shall manage the Web Development of the MC environment to include the following:

- Create, maintain and improve functionality on large scale websites and web-based applications.
- Follow the full life cycle software development process.
- Write efficient, well-documented code while keeping security and scalability in mind.
- Define new product requirements and features based on input from: Product Managers, System Administrators, and Network Engineers.
- Experience developing highly-scalable asynchronous web applications using JavaScript, HTML5 and CSS technologies
- Provide an in-depth knowledge of HTML5 and CSS3 for creating standards-compliant websites
- Develop web applications with PHP utilizing open source software (i.e. MySQL databases)
- Provide experience with modern JS libraries such as jQuery, and front-end JS application frameworks such as Angular or Ember
- Design and debug for cross-browser compatibility (internet explorer, Firefox and chrome).
- Define critical web-based security vulnerabilities and exploits based on Open Web Application Security Project (OWASP) or other like security standards- keeping current IAW security requirements.
- Familiarity with multiple code management techniques.
- Work independently and collaborate with non-technical and technical colleagues.

3.3 HELPDESK SUPPORT

The contractor shall support the following systems as helpdesk operations:

- Joint Battle Command – Platform (JBC-P)
- Joint Capabilities Release (JCR)
- Blue Force Tracking 1 (BFT1)
- Blue Force Tracking 2 (BFT2)
- PM Tactical Networks
- PL-NET E
- Other PEO-C3T Systems

In the future, additional systems may be added. Helpdesk support is required on site 24 hours per day,7 days per week. The Helpdesk Tier Structure is defined as follows and shall support all systems under the purview of PEO C3T:

- Tier 1 – Initial contact with users; Gather information regarding user affected, serial numbers of affected portion of network (as applicable), complete description of problem, time problem occurred, time of resolution; Notification of problem to management per Standard Operation Procedures; Initiate and track trouble tickets through resolution; Provide user-level support and troubleshoot problem; escalate problem to next level per Standard Operating Procedure (SOP) if problem cannot be resolved

- Tier 2 – Troubleshoot and provide resolution to problems beyond the capability of Tier 1; Troubleshoot servers and adjust software parameters; Provide field level troubleshooting and support to users; Add entries to trouble tickets showing work done and support provided; escalate problem to next level per SOP if problem cannot be resolved

- Tier 3 – Troubleshoot and provide resolution to problems beyond the capability of Tier 2; Troubleshoot overall network and provide minor software changes; Provide lower-level depot troubleshooting and support for the network; Add entries to trouble tickets showing work done and support provided

(a) Helpdesk Support for JBC-P, JBC-P Joint Capabilities Release (JCR)

The contractor shall provide JBC-P and JBC-P JCR support. Support duties shall include the following:

- Provide support to PM MC, or designated representative(s) for operational readiness, hardware installations/de-installations, hardware/software changes, configuration management, security, and weekly reporting.
- Maintain site operations documentation. Document contents shall be in coordination with the BFT Product Manager. Documents include:
  - SOP's
  - Briefings
  - Description of specific operations concepts
  - Site and network architecture
  - Trouble reports/fixes
  - Changes in processes
  - Changes in operations Point of Contacts (POCs) at units supported
  - Configuration control
  - Operations
- Provide continuous training for any level 1 administrator as defined in Army Regulation (AR) 25-2.
- Monitor, operate and maintain the tactical servers and other computer systems associated with the JBC-P Operations Centers.
- Perform software and hardware systems repair, installation, de-installation and management of upgrades to the BFT operation center.
- Serve as liaison with Defense Information Systems Agency (DISA), Continental United States (CONUS) Theater Network Operations and Security Center (CTNOSC) and local NEC for system

status reporting and local and long haul information service requirements, as listed in JBC-P Operations Center SOPs and the Network Enterprise Center (NEC) operations SOPs.

- Support operational security requirements (OPSEC) for each location, and for the unique security requirements of servers within the JBC-P Operations Center. The Contractor shall support configuration management for software and hardware systems within the JBC-P Operations Centers.
- All incoming/replacement contractor personnel shall be trained on all systems necessary to provide operations for Tier 1, Tier 2, and Tier 3 for the JBC-P Operations Center. The contractor shall develop formal training material to include text material, slides and interactive training materials per the JBC-P Operations Center Program of Instruction and should have items available at the request of the Government.
- Provide help desk services for all JBC-P customers, both terrestrial and Satellite Communications (SATCOM) based. The contractor shall expeditiously respond to all user issues, questions and complaints. The contractor shall be responsible for forwarding of issues to personnel who are best qualified to resolve them. These conditions, as well as response time requirements, are spelled out in the JBC-P Operations Center SOP. MCSC contractor personnel will be required to contact the Radio Frequency (RF) L-Band satellite, Very Small Aperture Terminal (VSAT) and Internet services providers to expeditiously troubleshoot network outages

(b) Helpdesk Support for BFT-1

The contractor shall provide BFT-1 helpdesk support at the Tier 1/2/3+ levels, as defined above:

Specific support duties shall include the following:

- Monitor the BFT-1 network
- Provide production Over-the-Air (OTA) updates/re-provisioning to authorized BFT-1 transceivers, including OTA re-key and zeroize functions, immediately upon receipt of request.
- Perform transceiver software file generation for production profile and delivery to the field according to the BFT-1 data handling guidelines.
- Input new transceiver serial numbers into files at all MCSCs at Contractor and FBCB2/ JBC-P BFT-1 approved time windows.
- Coordinate manual switch over changes between BFT-1 L-band redundant channels
- Configure existing MCSC equipment to adjust for BFT-1 approved network change requests
- Work with other MCSC personnel to provide seamless service throughout the FBCB2/ JBC-P BFT-1 network.
- Pull data as requested.
- Monitor all host, network and security device logs and analysis of this data to maintain the security posture and status of the worldwide BFT-1 network.
- Troubleshoot servers and adjust software parameters.
- Provide field level troubleshooting and support to users.
- Add entries to trouble tickets showing work done and support provided.

- Escalate problem to next level per SOP if problem cannot be resolved.

(c) Helpdesk Support for (BFT-2)

The contractor shall provide BFT-2 helpdesk support at the Tier 1/2/3+ levels, as defined above:

Specific support duties shall include the following:

- Monitor the BFT-2 network
- Provide production Over-the-Air (OTA) updates/re-provisioning to authorized BFT-2 transceivers, including OTA re-key and zeroize functions, immediately upon receipt of request
- Perform transceiver software file generation for production profile and delivery to the field according to the BFT-2 data handling guidelines
- Input new transceiver serial numbers into files at all MCSCs at Contractor and FBCB2 /
- JBC-P BFT-2 approved time windows
- Coordinate manual switch over changes between BFT-2 L-band redundant channels
- Configure existing MCSC equipment to adjust for BFT-2 approved network change requests
- Work with other MCSC personnel to provide seamless service throughout the FBCB2 JBC-P BFT-2 network
- Pull data as requested
- Monitor all host, network and security device logs and analysis of this data to maintain the security posture and status of the worldwide BFT-2 network
- Troubleshoot servers and adjust software parameters;
- Provide field level troubleshooting and support to users
- Add entries to trouble tickets showing work done and support provided
- Escalate problem to next level per SOP if problem cannot be resolved

(d) Helpdesk Support for Host Based Security System (HBSS)

The contractor shall provide HBSS helpdesk support.

Specific support duties include the following:

- Plan, coordinate, and configure connectivity and user account access to all relevant Army Enterprise Theater ePolicy Orchestrator (ePO) servers
- Plan, coordinate, procure, configure, operate, and maintain the security posture of a sufficient quantity of HBSS Dedicated Remote Console (DRC) workstations to support management of all relevant Army Enterprise Theater ePO servers. DRCs only require use of the Internet Explorer browser application to perform their mission, and may be either thick or thin clients
- Ensure that all assigned HBSS support personnel complete DISA required 32-hour HBSS Administrator training. This training requirement will be satisfied by attending regularly scheduled

DISA HBSS classroom training sessions, or by completing the online computer-based training located at https://www.fedvte-fsi.gov

- Develop and maintain SOP and Tactics, Techniques and Procedures (TTPs) for all critical HBSS operations, administration, and trouble ticketing processes used to support operational units
- Manage, maintain, and organize all Tactical Unit and PM System Containers in the System Tree on all Army Enterprise Theater ePO servers per NETCOM System Tree Standards
- Monitor the effective baseline of all HBSS endpoint protection product software on all Theater ePO servers to ensure it is up-to-date with United States (U.S.) Army Cyber Command (ARCYBER) and U.S. Army Network Enterprise Technology Command (NETCOM) HBSS Change Control Review Board (CCRB) baselines requirements. Report discrepancies to the pertinent Regional Cyber Center (RCC) using the NETCOM trouble ticketing system
- Field, document, and respond to all Tactical Unit phone calls and/or trouble tickets submitted requesting assistance to resolve HBSS related technical configuration issues. For technical issues that cannot be resolved by the APG MCSC Help Desk staff, contact the on-call PdM WIN-T INC3 HBSS Technical Team member for technical support
- When requested by the field, conduct HBSS policy tuning on operationally fielded PM systems to resolve urgent technical issues affecting a Unit's operational mission.
- Make required changes to the ASA (ALT) HBSS policy baselines on Theater ePO servers, document, and forward to PdM Tactical Cyber and Network Operations (TCNO) (formerly known as Warfighter Information Network-Tactical Increment 3 (WIN-T INC3)) HBSS Technical Team for technical analysis, concurrence, and master policy baseline updates, as required
- Configure and monitor HBSS Dashboards on all Theater ePO servers that display and track HBSS compliancy status across the Army HBSS Enterprise for all Operational and Generating Forces. Provide weekly reports as required by ARCYBER, Assistant Secretary of the Army for Acquisition Logistics and Technology (ASA(ALT)), and PEO C3T headquarters (HQ)
- Generate weekly HBSS compliancy reports for all Theater Enterprise ePO servers, and coordinate with operational units to correct discrepancies (e.g., outdate Antivirus DAT files, missing HBSS modules, unauthorized policy settings, etc.)
- Configure and monitor HBSS Dashboards on all Theater ePO servers that display and track High Severity security events detected on PM systems across the Army HBSS Enterprise for all Operational and Generating Forces. Coordinate with operational units to correct discrepancies (e.g., virus outbreaks, intrusions, active exploits, unauthorized system changes, etc.) Provide daily/weekly reports as required by Army Cyber Command (ARCYBER), Assistant Secretary of th Assistant Secretary of the Army for Acquisition, Logistics, and Technology e Army for Acquisition, Logistics, and Technology ASA(ALT), and PEO C3T HQ.
- Coordinate with the PdM TCNO (formerly known as WIN-T INC)3 HBSS Configuration Management (CM) Manager to ensure the latest approved ASA(ALT) HBSS Global Policy Sets are available on all Theater ePO servers.
- Distribute periodic formal policy releases from the HBSS CM Manager to all relevant Theater Enterprise ePO servers.
- Coordinate with operational units to ensure that correct ASA(ALT) HBSS policies are assigned to the proper Unit Containers and/or PM systems.

- Coordinate and prepare Tactical units for initial HBSS training and implementation. Prepare Unit Containers on the Theater ePO server to receive Unit assets. Execute Unit-level implementation checklist to collect tactical network configuration information and process required Request for Change (RFC) and DD2875 documents with RCCs for DRC and SuperAgent Distributed Repository (SADR) connectivity, and ePO server user account establishment.

(e) Helpdesk Support for PD Key Enterprise Management (KEM)
The contractor shall provide PD KEM Tier 1support, which includes the following:

- Initial contact with users.
- Gather information regarding user affected serial numbers of affected portion of network (as applicable), complete description of problem, time problem occurred and time of resolution.
- Notification of problem to management per Standard Operation Procedures.
- Initiate and track trouble tickets through resolution.
- Create accounts and reset passwords.
- Provide user-level support and troubleshoot problem.
- Troubleshoot servers and adjust software parameters.
- Provide field level troubleshooting and support to users.
- Add entries to trouble tickets showing work done and support provided.
- Escalate problem to next level per SOP if problem cannot be resolved.

(f) Helpdesk Support for Data Dissemination Services (DDS) and Command and Control Registry (C2R)
The contractor shall provide DDS and C2R Tier 1-3 support, which includes the following:

- Develop and maintain in-depth knowledge of, and provide complete support for SMC Common Software products.
- Support customers on complex technical issues including problems related to enterprise networks, servers and workstations.
- Respond to requests and inquiries from users and field support representatives within the pre-determined timeframe of our service level expectations.
- Investigate and resolve problems installing software as a result of complex environmental variables including Virtual Machine Software (VMWare) and Windows Server.
- Identify solutions to work around open issues / problems that are under investigation or pending resolution.
- Document, and track, case histories, issues, and actionable steps taken.
- Improve documentation of support policies and procedures.
- Provided technical support training to other team members.
- Provide accurate, detailed and timely responses to problems and queries.
- Provide technical guidance and assistance to customers in troubleshooting, identifying, and resolving system and interface problems.
- Review installation documentations to verify Server Deployment success, and document recommended changes.

- Maintain detailed trouble ticket information using the existing Mission Command Support Center process database, assign proper severity levels, updating steps taken and issue resolution.

(g) Helpdesk Support for Command Post of the Future (CPOF)
The contractor shall provide CPOF help desk support, which includes the following:

- Maintain 24/7 on-call support for PM MC Systems, Field Service Representative(FSR) support and customer issues
- Provide telephonic sustainment and training support to customers as directed.
- Create draft Technical Bulletins that identify potential issues and opportunities to improve system reliability and submit to the Product Lead for the system for approval through the MC Change Control Board (CCB) process.
- Coordinate PM MC System's development and testing support as needed.
- Directly contact Forward team and customers to walk them through critical issue resolution.
- Provide field feedback to development and logistics from units and FSRs to identify improvements to increase system performance, usability and stability.
- Handle internal PM MC technical coordination (PM MC and Development team).
- Support QA/testing efforts by re-creating issues, testing potential fixes & performing upgrades and configuration changes in test environments prior to and post release.
- Support all PM MC Development, testing and training events.
- Utilize Government provided trouble ticket system (example: SIF IRM) and send out weekly updates to document activities and actions.

3.4. ENGINEERING SUPPORT

The contractor is required to provide engineering support to MC. Engineering support duties include the following:

- The contractor shall provide engineering support, analysis and technical support to PM MC, operations personnel and BFT personnel to address technical issues, support investigation and diagnosis of operational anomalies, and network troubleshooting. Support duties include the following:
  - Simultaneous forwarding system log and security alert logs of host, network and security devices to the primary MC Operations Center monitoring and analysis servers
  - Network and systems vulnerability assessment in association with MC-defined procedures
  - Configuration management of all network security-related devices and software, to include firewall, intrusion prevention, intrusion detection and anti-virus (both host and network-based)
  - Maintain network security-related performance data during the contract period of performance, to include all system and device configurations, system log and accounting data, security device reporting and alert logs, analytical results and reporting; Archive and maintain these data products IAW MC BFT-defined procedures
  - Insure all network and security devices, and their configurations, are kept current to allow the most secure network possible while allowing for proper operation; Insure Server Operating Systems are kept up to date and Information Assurance Vulnerability Alert (IAVA) compliant

  - Notify MC BFT of any hardware/software system limitations that would prohibit operating system upgrades/patches/updates
  - Recommend new hardware/software as needed
  - Recommend and implement configuration changes in conjunction with the MC BFT-defined procedures
- Provide engineering and technical support throughout the planning, installation, commissioning/decommissioning, and operation of each MC Operations Center in coordination with PM MC. Engineering support shall be provided for new MC Operations Center installations in coordination with PM MC and for new software and hardware improvements within the existing BFT network. This is intended to provide continued MC Operations Center optimization.
- Provide new hardware and/or software, replacement hardware, and miscellaneous materials as required to support continuous operations with the incorporation of new technologies in coordination with PM MC
- Ensure that all operational and test MCSCs that receive a feed from the satellite service provider shall have a secure Virtual Private Network (VPN) Connection protecting and maintaining the integrity and isolation of MC BFT data. The VPN connections made to the closed MC-BFT Test network shall be secured with the strongest and DoD approved network encryption in accordance with the PM MC data transmission guidelines.
- Ensure that data collected from the MC-BFT servers is secured with the best available commercial encryption whenever it is transferred from the system, in strict adherence with PM MC policies and procedures.
- Provide engineering support to the Product Lead, BFT Operations and the lead systems engineer. The contractor shall supply direct engineering support to MC Operations Centers as site leads/site engineers, represent BFT Operations in the absence of the Product Lead, BFT Operations, BFT Chief Engineer, or BFT Lead Systems Engineer, and provide repair/upgrade capability of MC Operations Center hardware and software at their assigned site .
- Provide technical and operational counsel as advisors of a BFT Operations Cell.

3.5 SATELLITE NETWORK OPERATIONS SUPPORT

Satellite Network Operations support will entail operational and monitoring support of the BFT satellite networks. Support duties shall include the following:

- Monitor of the Worldwide BFT satellite networks
- Monitor all host, network and security device system logs, security alert logs and provide analysis of this data to maintain the security posture and status of the worldwide BFT satellite networks
- Monitor access controls and individual system/device accounts across the managed portion of the BFT networks
- Monitor network and security events for any security-related anomalies to maintain the security posture and status of the worldwide BFT satellite networks
- Respond to satellite network security events IAW MC BFT-defined procedures

- Perform satellite network task changes to servers as required by the BFT MCSC Manager, BFT Chief Engineer, Lead Systems Engineer, or local Systems Engineer based on current situational requirements
- Monitor and maintain or replace hardware directly related to the satellite networks
- Provide help desk functions for the satellite networks to assist with troubleshooting network issues
- Document all help desk contacts within the MC/BFT Field Support Center website to detail issues reported, who reported the issue, unit with issue, location and complete history of issue being worked
- Elevate troubleshooting issues not capable of being corrected by local Network Administrator personnel
- Maintain the operational capabilities of the BFT-2 network equipment located at the Operations Centers (SNCC, MC Operations Center Client, and all VSAT equipment) and at the Satellite Ground Stations (SGS and VSAT)
- Maintain the operational capabilities of the BFT VSAT equipment located at the Operations Centers and the Satellite Ground Stations.

Operate, monitor, sustain and maintain all BFT VSAT equipment at all current and evolving locations worldwide.

3.6 IP NETWORK OPERATIONS SUPPORT

The contractor shall provide IP Network support services for network routers and security devices connected to the Comtech Network Packet Switch (NPS), ViaSat Satellite Network Control Center (SNCC), satellite networks, isolation routers, unclassified networks (both Government and commercial), and classified Government networks. Support duties shall include the following:

- Monitor and manage all network device configurations for all MC Operations Center Operations and Test events
- Monitor and integrate multi-domain network architecture for MC Operations Center operations and test events
- Provide network engineering support for BFT Operations in support of test events
- Provide network configuration management documentation to the program office in accordance with established regulations and policies
- Support System Accreditation and IAVA compliance on all MC Operations Center Servers and network devices
- Train site engineers and MCSC system administrators on MCSC networks and tunnels
- Provide input on documentation and instruction materials created for MCSC operations
- Provide assistance in developing fielding plans for network enhancements
- Recognize a potential network violations, report the incident, and mitigate any adverse action
- Support, monitor, test, and troubleshoot hardware and software problems pertaining to their Computing Environment
- Install and operate the IT system in a test configuration manner that does not alter the program code or compromise security safeguards

- Test Information Assurance (IA) safeguards in accordance with established test plan and procedure
- Apply appropriate access controls and established IA security procedures and comply with responsibilities of assignment
- Implement applicable patches including IAVA for network devices
- Analyze patterns of non-compliance and take appropriate administrative or programmatic actions to minimize security risk
- Analyze system performance for potential network problems
- Configure, optimize, and test network services, hubs, routers, and switches to ensure they comply with security policy, procedures, and technical requirements
- Install, test, upgrade, and maintain network operating systems software and hardware to comply with IA requirements
- Plan and schedule repairs as required
- Plan and schedule the installation of new or modified hardware, operating systems, and software applications
- Design network architectures including firewalls, routers, switches and other network systems as directed by Program Manager
- Operate, monitor, sustain and maintain all BFT interface equipment at all current and evolving locations worldwide connecting to the internet provider

3.6.1 ENTERPRISE ARCHITECT

The following tasks are required in support of the Blue Force Tracking Global Network (BGN) and the National Enterprise Data Portal (NEDP):

- Design, plan, monitor and maintain the architecture that enables the Blue Force Tracking Global Network (BGN) to be the most secure, reliable and efficient hosting infrastructure for Army tactical systems
- Analyze system requirements to properly allocate hosted system processing capacity and memory utilizing the most efficient algorithms and resource provisioning provided by the latest VMWare system components
- Constantly monitor network bandwidth utilization, growth trends and planned capacities to meet both planned and unknown future system requirements
- Design and manage network and local data storage solutions utilizing advanced storage tiers, shared data blocks and snapshot technology. Monitor and plan for future storage needs while making the most efficient use of current capacity by continually de-duping and reclaiming space
- Insure full redundant power in the data center for all physical hardware while designing architecture to minimize power consumption. Monitor consumption trends, balance loads and plan for increases where required
- Determine heat load of data center devices and insure proper cooling, airflow and efficient layout are maintained for all devices and racks
- Provide robust and flexible voice services to the BGN and hosted organizations, including inbound call routing, queuing, voice messaging, local quality of service, conferencing and other advanced phone features

- Create and continually review BGN specific device policies. Create and maintain baseline configuration database for all network devices. Dynamically review baseline configurations against DoD security technical implementation guides and industry best practices and make changes where appropriate for environment. Perform near real-time review of all configuration changes that differ from BGN establish baselines
- Design secure and efficient networks for multiple enclaves and simultaneous test events using advanced dynamic routing configurations such as policy based routing, route-map distribution, network address translation and virtual routing and forwarding enabling the BGN to support multiple isolated events in the same physical infrastructure. Provide advanced network security configurations in both the physical and virtual environments. Design secure one-directional live data feed channels for test and shadow enclaves
- Provide expert network troubleshooting for complex issue both in the BGN networks and with remote partner networks utilizing advance packet capture and analysis techniques. Design secure and robust remote access solutions for remote partners and BGN staff
- Perform security and design review of architectures provided by system vendors and enhance them to work more efficiently and securely at the BGN and on real-world networks. Design additional solutions for deployment plans that may have been missed such as integrated authorization and authentication components
- Maintain detailed network diagrams reviewed and updated at least weekly in response to continually changing network components, test events, system capabilities and requirements from the Government. Provide network architecture designs with logical and dataflow diagrams suitable for various audience levels. Create network policy and Tactics, Techniques & Procedures (TTP) documents
- Perform in-depth research of capacities of new system components, gather additional requirements from stakeholders and research possible alternative off-the-shelf solutions. Perform proactive analysis of current systems and emerging technologies to make recommendations to Government
- Maintain dynamic monitoring and tracking of all devices and systems allowing for preemptive capacity and maintenance planning. Track and plan for device and system full life-cycle to reduce risk of operating on less efficient or out of support equipment. Perform continuous security posture evaluation through components complete life cycle at BGN
- Design, secure and maintain robust authorization and authentication components leveraging multiple technologies such as Active Directory, LDAP, Remote Authentication Dial-In User Server/Service (RADIUS), Kerberos and Terminal Access Controller Access-Control System Plus (TACACS+)
- Create and maintain complex operational scripts to dynamically control network components and routing such as BGN tactical change-over and phone change scripts
- Perform historic trouble analysis, predictive risk assessment and proactive planning to mitigate the operational effect of likely future issues or potential system failures.
- Continually track vendor software feature, security and bug-fix releases to proactively patch before issues are release as IAVA. Evaluate new software releases in controlled test environment and analyze impact to BGN networks and operations

3.7 SECURITY ENGINEERING SUPPORT

The contractor shall provide Security Engineering support services for security devices supporting all connections to the MC Operations Center and network connection required by the Government. Support required includes the design and implementation of firewalls, intrusion detection systems, intrusion prevention systems; implementation of Security Information Management (SIM), McAfee Host Based Security System (HBSS), LINUX security and Windows security. Support duties shall include the following:

- Monitor and integrate multi-domain network architecture for MC Operations Center operations and test events
- Provide configuration management documentation to the program office in accordance with established regulations and policies
- Support System Accreditation and IAVA compliance on all MC Operations Center Servers and network devices
- Trains site engineers and MCSC system administrators on Intrusion Detection System (IDS) and HBSS
- Provides input on documentation and instruction materials created for MCSC operations
- Provides assistance in developing fielding plans for new security enhancements
- Recognize a potential security violation, report the incident, and mitigate as necessary
- Support, monitor, test, and troubleshoot hardware and software Information Assurance (IA) problems pertaining to their Computing Environment
- Install and operate the IT system in a test configuration manner that does not alter the program code or compromise security safeguards
- Conduct tests of IA safeguards in accordance with established test plan and procedure
- Apply appropriate access controls and established IA security procedures and comply with responsibilities of assignment
- Implement applicable patches including IAVA for their Computing Environment operating system(s)
- Analyze patterns of non-compliance and take appropriate administrative or programmatic actions to minimize security risk
- Analyze system performance for potential security problems
- Configure, optimize, and test network services, hubs, routers, and switches to ensure they comply with security policy, procedures, and technical requirements
- Install, test, upgrade, and maintain network operating systems software and hardware to comply with IA requirements
- Install perimeter defense systems including IDS, firewalls, grid sensors, etc. and enhance rule sets to block sources of malicious traffic
- Plan and schedule repairs as required
- Plan and schedule the installation of new or modified hardware, operating systems, and software applications ensuring integration with IA security requirements, for the enclave
- Analyze IA security indicates and patterns to determine remedial actions to correct vulnerabilities.
- Design perimeter defense systems including IDS, IPS, firewalls, grid sensors, etc. and enhance rule sets to block sources of malicious traffic
- Creating a proactive security posturing and rapid response to threats

3.7.1 COMPUTER FORENSIC AND INTRUSION ANALYST

- Maintain currency of knowledge with all IA-applicable DoD / Defense Information Systems Agency (DISA) / National Intelligence Support Team (NIST) and Army regulations, instructions and orders as they pertain to the BGN network
- Perform gap analysis across the organization to identify and document unnecessary complexity in existing processes and procedures; work with service and application owners on mitigation strategies
- Act in an advisory role in application development and acquisition to assess security requirements and controls and to ensure that security controls are implemented as planned
- Create and publish BGN security policies that incorporate all facets of the DoD / DISA / Army policy structure, and are directly applicable to the BGN network environment specifically
- Provide analytical and technical security recommendations to other BGN team members, vendors (ViaSat, Comtech), other programs who are utilizing the BGN network (Global Command and Control System - Army (GCCS-A), S2MC, DDS, C2R, C2I Virtual Machine, Zero 2 (Z2) Technologies Webservers), and the Government. Identifies requirements, based upon need or as the result of a security issue that puts Government systems at risk. Assess the effectiveness of vendor / other non MC / Mission Command (MC) programs information protection measures as utilized within the enclave
- Provide analytical and technical security recommendations for third-party hosting of additional DoD programs that leverage the BGN network environment for service hosting. This includes system risk analysis, data profiling, vulnerability testing and redesign of security safeguards to accommodate the new systems
- Provide Subject Matter Expert (SME) / briefing / technical writing services to the PM MC Information Assurance personnel (IAM, IASO, Cyber Security Branch) for all DoD / DISA / Army security policies, instructions and programs, to include (but not limited to) Host Based Security System (HBSS) / Intrusion Detection System (IDS) / Application Control Architecture Services (ACAS) and their current deployment status
- Provide penetration testing in advance of test events and outside audits; supervise and provide active protect, detect, react and respond (PDRR) as well as active / passive network defense (CND) services during test and evaluation activities
- Serve as the Information Assurance (IA) / Cybersecurity Subject Matter Expert (SME) leader embedded in the BGN, by staying abreast of business and industry technologies and trends; evangelize IA / Cybersecurity to BGN personnel
- Design IA architectures and designs for DoD Information Systems with high integrity and availability requirements, to include Mission Assurance Category (MAC) I systems and designs for systems and networks with multilevel security requirements or requirements for the processing of multiple classification levels of data (e.g., UNCLASSIFIED, Critical Unclassified Information (CUI), and SECRET)
- Ascertain new and older non-IAVA released vulnerabilities as they pertain to BGN network devices, servers and websites. Remediate / Mitigate and document as found
- Provide mentoring and technical leadership to the Information Assurance System Architect and Engineer (IASAE) and Information Assurance Training (IAT) Level I and II personnel, coordinate and

supervise appropriate IT staff to implement solutions which will meet or exceed Government expectations and design, publish, and uphold standards for monitoring critical security indicators in the BGN Mission Command Support Center

- Research and recommend tools to help manage security analysis, process, and risk. Design, develop, and supervise implementation of specific IA countermeasures for the enclave.
- Design security standards, methodology framework, and monitors for risks and/or effectiveness; evaluate and acquire technology to automate security monitoring
- Act as SME to provide support and analysis during and after security incidents, to ascertain the scope of incident and apply the Incident Response Plan as the primary Point of Contact (POC), as required.

3.8 TEST EVENT AND TRAINING SUPPORT (FFP)

The contractor shall support current and future DOD test events and unit tests in software fielding and feasibility assessment of new capabilities. This support entails creating detailed network architectures, designing high level data flows, providing systems engineering and best business practices in the integration of MC BFT capabilities with Non-MC BFT systems, configuration management, risk management, requirements engineering, executive reporting, test reporting and incident tracking. The contractor must be able to support, at a minimum, (12) simultaneous test events. If a test event requires 24-hour support, the contractor shall support. The contractor shall maintain a Program of Instruction (POI) for initial standardized training of contractor employees for the duration of this task order. The POI shall encompass the following:

- Standard operation of MC Operations Center servers
- System connectivity, data flow, and application of software patches and upgrades
- All software and hardware for the fielded MC systems
- Instructional documentation for new or upgraded software versions quarterly or as required

3.9 SOFTWARE DEVELOPMENT SUPPORT

The contractor shall be part of a team with JBC-P software (SW) developer (currently the Software Engineering Directorate) for the evolution of the Network Operations Center (NOC) software to support additional versions of JBC-P, Mounted Computing Environment software as well as future BFT satellite communication initiatives.

The NOC SW serves as the central traffic and network management hub for Situational Awareness (SA)/Command and Control (C2) traffic from BFT platforms for Army, USMC and other joint partners. The NOC SW processes and routes messages over BFT and UTI/USMC networks. It supports multiple security domains and interoperability with Command Post systems.

The vendor shall provide support in the following areas: Systems Engineering, Information Assurance, Development, Integration and Testing of NOC SW. New capabilities must be tailored for Disconnected, Intermittent and Limited (DIL) bandwidth conditions.

Support may include:

- Additional data exchange formats (XML, sync) and reduce dependency on VMF.
- OTA SW updates/Patch management

- Identity management and Tactical PKI
- Platform HW reporting & management
- Redundancy and fault detection for SW/HW components
- Failover for service between available networks such as BFT, WIN-T, MUOS, etc.
- Ability to set SA/PLI to secret per region/COCOM
- Improved Cyber
- File transfer mechanism
- Network & System Monitoring and Management
- Collect and document NOC functionality

3.10 GOVERNMENT DIRECTED OVERTIME/SURGE (OPTIONAL) Labor Hour (LH)

During the course of performance the Government may require the Contractor to work 'on call' overtime hours and/or provide surge labor resources to support additional requirements, while continuing to provide standard contracted services. Optional Government directed overtime or surge support may apply to any of the tasks under section 3.0 of this Task Order.

For proposal purposes, the NTE value of these services is $500,000 per year. This work shall be proposed and billed on a Labor Hour basis.

3.10.1 Government-Directed On Call Overtime:

All Operation Centers require 24/7 365-day coverage. In some circumstances, on call overtime may be necessary for any PWS task and may require contractor personnel to report to the Government work locations outside of their normal work hours/shift in support of unanticipated events or requirements. Government directed overtime should only be used when all other possibilities have been exhausted. Overtime costs shall not be incurred unless authorized by the APG Contracting Officer's Representative (COR) with prior notification to the GSA Contracting Officer (CO) and the GSA COR. Sufficient funding must be available to cover incurred expenses. In the event of an afterhours emergency requiring immediate contractor support, APG may authorize (and will track) overtime costs up to $15K per month.

At the time of exercising overtime support the Government will:

- Identify the event (exercise/operation/project) which is driving the overtime requirement
- Identify the specific services where overtime or surge is authorized
- Define level of effort expectations (i.e. 12-hour days, 6 days per week)
- Identify duration or end date when overtime is no longer required
- Provide an estimate on the number of overtime hours required

3.10.2 Surge Requirements:

The Government may require the contractor to provide additional 'surge' labor support for additional within-scope requirements, while continuing to provide standard contracted services. The Government will define such requirements in advance, and the contractor shall submit a revised proposal for the Government's consideration that incorporates the necessary additional resources to perform the work. Any additional surge support will be proposed and billed on a Labor Hour basis, and will be incorporated into the task order via modification.

Both Government Directed Overtime, and Surge Requirements, shall be invoiced and tracked on a Labor Hour basis against the proscribed annual NTE amount.

4.0 Task Order Transition

The incoming and outgoing contractors shall work together, in collaboration with the Government, to rationalize Transition-In and Transition-Out Plans to effect a transition that provides for smooth operational turnover and minimizes operational impact to supported organizations.

4.1 Transition-In Plan

C Contractor shall prepare, for review and approval of by the Government, a Transition-In Plan that includes a schedule depicting the transition activities and milestones for accomplishing the Task Order transition. The transition-in period shall be no more than 30 days to 45 days.

The Contractor shall perform the following activities during the transition-in period. It is expected that weekly status meetings with all pertinent stakeholders at a mutually agreed upon day and time will be conducted, and that joint status meetings with pertinent stakeholders will be held at a mutually agreed upon dates and times.

- Perform joint inventories and inspections of all furnished facilities and property collaboratively with the Government and the outgoing contractor
- Perform joint identification and inventory of all contractor- maintained classified data, equipment and devices relevant to the performance of the contract, to ensure that proper accountability and chain of custody is maintained for all Communications Security (COMSEC) sensitive items
- Develop and validate a comprehensive communications and IT supported equipment list with the Government and outgoing contractor
- Coordinate with the Government to validate or establish Mission Assurance Categories (MAC) and maintenance priorities for supported equipment
- Establish procedures with the outgoing contractor to transition operations, maintenance, and logistics functions while maintaining an uninterrupted continuity of services without a

degradation of service. This includes defining processes for turnover of system administration, accounts, privileges, and access

- It is anticipated that weekly status meetings with all pertinent stakeholders at a mutually agreed upon day and time will be conducted

It is anticipated that joint status meetings with pertinent stakeholders will be held at a mutually agreed upon dates and times.

4.2. Transition-Out Plan

The contractor shall provide a seamless transition to the successor contractor personnel at the conclusion of this task order. The contractor shall provide a Transition-Out Plan not later than (NLT) 60-days prior to the expiration of the final exercised task order performance of period. The contractor shall identify and support transition activities, schedules and milestones for turnover of work centers/functions and shall coordinate with both the incoming contractor and the Government to transfer knowledge in the following areas:

- Project management processes
- Points of contact
- Location of technical and project management documentation
- Status of ongoing technical initiatives
- Transition of personnel
- Establish and maintain effective communication with the incoming contractor/Government personnel for the period of the transition
- Inventory, inspection and transfer of IT software and hardware, licenses, and warranties
- Inventory, inspection and transfer of all contractor maintained classified data, equipment and devices, ensuring positive control, accountability, and chain of custody is maintained for all COMSEC sensitive items
- Technical artifacts and configuration baselines
- Elevated system privileges
- Operations, maintenance, helpdesk, engineering and logistics functions
- Mission Assurance Categories (MAC) and maintenance priorities for supported equipment
- SOP Guidelines developed under TO
- Tracking databases for tickets

5.0 DELIVERABLES

Deliverable	PWS Reference	Title	Subtitle	Distribution	Required Time Frame
1	3.1	Contract Status Report	Contract Progress, Status and Management Reporting	COR	Monthly, 30 days after contract award
2	3.2	Scientific and Technical Reports Summary	Monthly Status Report	COR and MCSC Government leads	Monthly, beginning 10 calendar days after the first business day of the month following award.
3	3.2.1	Management Plan	Server Management Plan	COR and MCSC Government leads	30 working days after completion of study. Final do 30 working days after receipt of Government comments.
4	8.0	Scientific and Technical Reports Summary	Security Certification and Accreditation Plan	COR and MCSC Government leads	Initial due 90 days after Contract Award and final 30 working days after receipt of Governments comments.
5	6.1.3	Scientific and Technical Reports Summary	Misc. Reports	COR and MCSC Government leads	As required
6	3.4	Scientific and Technical Reports Summary	Systems Engineering Studies	COR and MCSC Government leads	30 working days after completion of study. Final do 30 working days after receipt of Government

					comments.
7	9.0	Performance and Cost Report	Performance and Cost Report	COR and MCSC Government leads	As required
8	3.1	Conference Minutes	Meeting Minutes	COR and MCSC Government leads	Initial 10 working days after meeting completion and final due 5 working days after receipt of Government comments.
9	4.1	Transition-In Plan		COR and MCSC Government leads	Due at proposal submission
10	4.2	Transition-Out Plan		COR and MCSC Government leads	NLT 60-days prior to end of final performance period, or as otherwise directed by the COR

6.0 CONTRACT MANAGEMENT/CONTRACTOR STAFFING

6.1.1 QUALITY ASSURANCE SURVEILLANCE PLAN (QASP)

The Government will utilize a Quality Assurance Surveillance Plan (QASP) to monitor the quality of the Contractor's performance. This oversight will help to ensure that service levels reach and maintain the required levels throughout the task order period of performance. The QASP also provides the COR with a proactive way to avoid unacceptable or deficient performance, and provides verifiable input for the required Contractor Performance Assessment Reporting System assessments. . The QASP will be finalized immediately following award and a copy provided to the Contractor. The QASP may be updated by the Government as necessary. The Government will also review the Monthly Progress and Quality Reports and will attend regular work performance review meetings with the Contractor to survey quality of products and services.

The MC COR is responsible for the following:

- Reviewing and certifying Contractor invoices for accuracy and validity.
- Monitoring performance, reviewing and approving task performance.
- Inspection and acceptance of deliverables.

The GSA COR, in collaboration with GSA Invoice Support Staff, will review the labor, travel, and ODC expenditures reflected in the Contractor's invoices.

The GSA COR, in collaboration with GSA Invoice Support Staff, will ensure that the ceiling and funded value of the task order and line items are not exceeded in the areas of labor, travel, and ODCs.

The PM MC COR will provide surveillance for each PWS task, reviewing deliverables for conformance to requirements. Services, deliverables, and reports that conform to Task Order requirements will be accepted. The GSA COR will periodically consult with the PM MC COR concerning the acceptability of services. The PM MC COR will notify the Contractor in writing, or verbally when warranted, of the need for corrective action when work does not comply with the Task Order requirements. If corrective action does not result in conformance to requirements, the GSA COR or GSA CO will be apprised of items that remain at variance with requirements. The Government will document overall satisfaction with Contractor performance through completion of a Contractor Performance Assessment Report (CPAR) on an annual basis prior to exercising an option, and this will be uploaded into the Contractor Performance Assessment Reporting System at www.cpars.gov.

In accordance with the Quality Assurance Surveillance Plan, the Government will document overall satisfaction with Contractor performance through review and evaluation of the Contractor's success in meeting the standards and measures outlined in the performance metrics table below.

6.1.2 PERFORMANCE REQUIREMENTS SUMMARY

The Government will monitor the Contractor's performance in accordance with the Quality Assurance Surveillance Plan (QASP) described above, and will use the Performance Requirements Summary (PRS) outlined below to evaluate whether the Contractor's performance is satisfactorily meeting the standards specified. While the table states that incentives may consist of positive past performance evaluations, it should be understood that failure to meet the performance metrics below will result in negative past performance evaluations. Past performance evaluations will be submitted to the Contractor Performance Assessment Reporting System (CPARS) for all Government agencies to review. Past performance evaluations will contain narratives explaining reasons for positive and negative evaluations.

Requirement	Acceptable Quality Levels	Methods of Surveillance	Impact if AQL is not met
24/7 365 coverage at all operation centers	100%	Completing periodic Inspections and Customer complaints	A delay in monthly or payments until deficiency is corrected and/or a monthly report that reflects deficiencies that may be reflected in CPARS system for performance
Completing all requirements specified on the Deliverables Table	100%	Verifying that all Deliverables are submitted by the date specified in the PWS or the date agreed upon by the COR	A delay in monthly or progress payments until deficiency is corrected and/or a monthly report that reflects deficiencies that may be reflected in CPARS system for performance
Maintaining Network stability in conjunction with other team partners	99.50%	File reviews, periodic inspections, and customer complaints	A delay in monthly or progress payments until deficiency is corrected and/or a monthly report that reflects deficiencies that may be reflected in CPARS system for performance
Resolve (or refer if above Tier Level 2 Capabilities) 95% of all tickets generated and received within 24 hrs of it being reported at the Tier 1 and Tier 2 levels	95%	A random sampling of Tickets will be reviewed to determine if required tasks was met. The 95% of the pulled tickets should meet the required tasks. Customer complaints within that month will be counted as part of the random sampling	A monthly report that reflects deficiencies that may be reflected in CPARS system for performance

Resolve or refer (to the next level) 95% of all tickets generated and received within 48 hrs of it being reported at Tier 3	95%	Same method as above (random sampling and customer complaints)	A monthly report that reflects deficiencies that may be reflected in CPARS system for performance

6.1.3 MONTHLY STATUS REPORT (MSR)

The Contractor shall develop and provide a Monthly Status Report using common office productivity suite applications which is due by the 15th of each month. The MSR shall be provided to the MC COR and the GSA COR via email, and shall be attached to the monthly invoice when submitted in GSA’s IT-Solutions Shop (ITSS) for payment. Information included in the MSR shall be segregated in accordance with a Government-approved format. The MSR shall include the information shown below. (The content may change over the course of the task order based on the needs of the Government.)

a. Activities during reporting period, by task (include on-going activities, new activities, activities completed; and progress to date for all covered activities). Start each section with a brief description of the task.
b. Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them.
c. Summary of trips taken, conferences attended, etc. Attach trip reports to the MSR for the reporting period.
d. Accumulated invoiced cost for each CLIN up to the previous month.
e. Projected cost of each ODC and Travel CLIN for the current month and forecasts through the end of the current performance period.
f. Comparison data / monthly performance reports.
g. Track and report on the basis of the type of funds being used.

The Monthly Status Report shall include an appendix that contains a staffing matrix in a format approved by the Government (shall be provided post award) that shows all positions by location, including:

a. currently filled positions
b. vacancies, personnel gains/losses and status (e.g., interview, offer pending, clearance pending, start/end dates, etc.)
c. other open positions that the Government has not authorized the Contractor to fill

6.1.4 BUSINESS/ACQUISTION MANAGEMENT

Organizational Conflict of Interest: Contractors are advised that performance of some tasks under this PWS may create an organizational conflict of interest that could restrict the Contractor from being able to compete on future acquisitions. See **’ATTACHMENT 6**’ in the RFP for the Organizational Conflict of

Interest (OCI) certification statement applicable to this task order.

6.2 CONTRACTOR STAFFING

Throughout the performance of this task order the Contractor shall provide and maintain qualified personnel who possess the requisite technical skills, qualifications, and experience together with the necessary program management and administrative support to meet the Government's requirements.

The Contractor shall provide Core Support for the tasks identified in PWS inclusive of sub-sections.

6.2.1 LABOR LEVEL OF SUPPORT

The Government anticipates staffing all of the Core Support positions reflected **in "ATTACHMENT A.1: Sites, Functions, Skill & Support Staff Requirements Table"** upon award of the task order.

6.2.2 CONTRACTOR KEY PERSONNEL

Contractor Key Personnel positions are identified in **"ATTACHMENT A.2: Top Secret and Key Personnel Positions"**. The Contractor shall not remove or replace any personnel designated as Key without the written concurrence of the PM MC COR and GSA CO. Replacement Key Personnel shall hold qualifications equal to or greater than the individual being replaced.

The Contractor shall submit written notification of proposed Key Personnel replacements no later than 14 calendar days prior to departure of the incumbent. This notification shall include the resume of the proposed substitute and shall include justification for the replacement in sufficient detail to permit evaluation of the impact of the change on Task Order performance.

If the Government determines that the proposed substitute personnel is unacceptable, or that the reduction of effort would be so substantial as to impair the successful performance of the work under the Task Order, the substitution will be denied and the Contractor shall propose an alternate candidate.

7.0 ADMINISTRATIVE CONSIDERATIONS

7.1 GOVERNMENT POINTS OF CONTACT

GSA PM/COR:
Shail Shah
GSA Federal Acquisition Service (3QSBC)
The Dow Building / 100 S Independence Mall West
Philadelphia, PA 19106
Voice: 215-446-5858
Voice: 215-446-5858
Email: shail.shah@gsa.gov

GSA Contracting Officer
Christine Chaapel
GSA Federal Acquisition Service (3QSBC)
The Dow Building / 100 S Independence Mall West
Philadelphia, PA 19106 Phone: 215-446-4898
Voice: 856-513-5399
Email: christine.chaapel@gsa.gov

GSA Contracting Specialist:
Thomas McCarthy
GSA Federal Acquisition Service (3QSBC)
The Dow Building / 100 S Independence Mall West
Philadelphia, PA 19106 Phone: 215-446-5868
Voice: 215-446-5808
Email: thomas.mccarthy@gsa.gov

PM MC Program Manager
(b) (6)
Client Acquisition Branch Chief
(b) (6)
[redacted]
Office: (b) (6)
Email: (b) (6)

PM MC Client COR:
(b) (6)
Acquisition Management Specialist
(b) (6)
[redacted]
Voice (b) (6)
Email (b) (6)

7.2 ORDER TYPE

The resultant Task Order will be a Hybrid Firm Fixed Price/Labor Hour order type which includes cost-reimbursable line items for travel and non-travel ODCs.

All labor task requirements will be awarded on a Firm Fixed Price basis with the exception of 3.10 Government Directed Overtime/Surge, which shall be awarded on a Labor Hour basis.

The task order may be incrementally funded in accordance with DFARs clause 252.232-7007, “Limitation of Government’s Obligation,” included herein.

7.3 PERIOD OF PERFORMANCE

The task order period of performance includes a twelve-month base period followed by four consecutive twelve-month options.

7.4 PLACE OF PERFORMANCE

All contractor work shall be performed at the following Government sites:

Primary sites:

- Aberdeen Proving Grounds, MD
- Fort Carson

Contingency Operational sites:

- Fort Hood, TX – This is a contingency operational site in case of an emergency at either of the Primary Government sites. The contractor shall provide support at Fort Hood, TX as stipulated by the Government.
- Other Government locations and/or contingency sites may require contractor support by PM MC and may be identified at a later time.

7.5 WORK HOURS

FTE (Full-time Equivalent) - An FTE is defined as working 40 hours per week, 160 hours per month, 1920 hours per year. Core hours are between 9am – 5pm local time, Monday through Friday excluding federal holidays (at 8 hours per day, 5 days a week, 52 weeks a year).

Out of Hours Work / Overtime - For the Helpdesk, the Government requires on-site contractor support 24 hours per day, 7 days per week and 365 days per year support including holidays and weekends. The contractor shall provide personnel to support three 8-hour shifts per day to sustain this schedule at the Government work locations.

The contractor may be required to work outside these hours to satisfy Government requirements for a variety of situations, including emergencies, training exercises, testing, or other mission priorities. (See PWS Section 3.10.) It is expected that the contractor, based on its corporate policy, will compensate its staff through offset/credit hours or other measure for hours worked outside the normal duty time. When the overtime requirement exceeds the standard pay period, prior authorization by the PM MC COR is required. Deviations to these stipulations, as well as deviations to the normal work day schedule, must be authorized in advance by the MC COR or their designee.

7.6 TRAVEL and NON-TRAVEL OTHER DIRECT COSTS (ODCs)

Not-to-exceed ceiling values for Travel and Non-Travel ODCs have been established for each period of performance. Travel and Non-Travel ODCs will be invoiced on a cost-reimbursable basis.

TRAVEL:

CONUS and OCONUS travel may be required during the course of task order performance. The Contractor shall visit sites as required by the Government and directed by the PM MC COR to accomplish tasks associated with performing services under this task order. Travel may be required to support activities such as system integration, fielding equipment, troubleshooting, and conducting training on systems covered within the scope of this PWS. The Contractor shall make its own travel arrangements. All reimbursable travel shall be pre-approved in writing by the PM MC COR. The Contractor shall not be reimbursed for travel within a 50-mile radius of contractor personnel's assigned duty station.

The Contractor shall ensure that all travel is in accordance with the Joint Travel Regulations (JTR). Maximum use is to be made of the lowest available customary standard coach or equivalent airfare accommodations available during normal business hours. If available, the contractor is authorized to fly on scheduled and non-scheduled military aircraft when associated with testing or in the overall performance of this contract. The Contractor shall be limited to renting compact cars, all hotel billings will be within the Government per diem rates, and all airline flights will use non-reimbursable tickets using Government city pairings.

The Contractor shall keep a summary of all long-distance travel, to include, at a minimum, the name of the employee, location of travel, duration of trip, and POC at travel location.

When multiple Contractor personnel travel to same site a single vehicle must be utilized. This policy will be strictly enforced and any deviations must be pre-approved by the PM MC COR.

NON-TRAVEL OTHER DIRECT COSTS (ODCs)

ODCs may include hardware, software, and equipment required to support continuous operations, the incorporation of new technologies, technology refresh periods, security and mission as required by the Government. Such requirements will be identified at the time the Task Order is issued or may be identified during the course of the task order by the Government or the contractor. All contractor acquired ODCs will be Government owned and Government licensed, if required, prior to being utilized in support of this requirement.

Travel and ODCs will be invoiced on a cost-reimbursable basis.

Non-Travel ODC items having a total procurement cost over $10,000 shall have the written approval of the PM MC COR and the GSA Contracting Officer prior to purchase. For purchases over the DoD micro-purchase threshold of $5000 the contractor shall obtain three competitive quotes, or provide the rationale for a single source procurement, and shall be prepared to provide backup information at the Government's request.

If the contractor initiates the purchase at a total procurement cost over $10,000 and has an approved purchasing system the contractor shall submit a 'Request to Initiate Purchase' form (RIP) to the PM MC COR and the GSA COR. If the contractor does not have an approved purchasing system, a 'Consent to Purchase' form (CTP) shall be submitted to the GSA CO and COR. The RIP or CTP document shall include the purpose, specific items, estimated cost, cost comparison, and rationale for purchase. The contractor shall not make any purchases without an RIP that has been approved by the PM MC COR, GSA COR, and GSA CO. The anticipated time frame for approvals is 3 to 5 business days.

Federal contracting laws and regulations apply to all Contractor open market purchases of materials and equipment under this task order. Prices must be determined fair and reasonable from competitive sources and are subject to Government audit. The Contractor shall maintain records for all ODC purchases documenting competitive sourcing, or the rationale for single-source procurement if necessary, in strict compliance with the competition requirements set forth in the Federal Acquisition Regulation (FAR), and shall provide copies of all such documentation upon the Government's request to verify compliance. The Contractor shall only be permitted to apply indirect rates to ODC purchases after award if such application is consistent with the successful price proposal and DCAA recommendations. No profit or fee shall be allowed on ODC costs.

All ODC items purchased by the Contractor for the use or ownership of the Federal Government shall become property of the Federal Government. If the Contractor acquires hardware or software maintenance support, all licenses and/or contractual rights to receive title shall be turned over to the Government upon completion of the task order. The Government's liability to reimburse the Contractor for costs incurred from the acquisition of hardware/software maintenance support shall be limited to costs incurred during the period of the order for which the Government received the items acquired.

7.7 GOVERNMENT FURNISHED EQUIPMENT/MATERIALS FACILITIES

PM MC and PEO C3T programs will provide necessary test equipment to perform testing and providing support on their respective systems. The Government will provide the contractor records of all Government-owned property and equipment that are under warranty and used, managed, or supported under this task order. The Government shall provide office space, furniture, computer equipment, telephone, and reproduction facilities for employees working at Government facilities in support of this effort. All equipment purchased and received as Government Furnished Equipment (GFE) will be accounted for in accordance with Government approved internal property controls. The contractor shall provide a GFE/GFI Quarterly Report within the Monthly Status Report (only needed 4 times per year) that tracks the GFE/GFI. The contractor shall maintain copies of warranty records for Government-owned property and provide the records and the property to the Government when requested, or at the conclusion of the contract. The contractor shall be responsible for security of all keys and access cards provided by the Government. These controls will be established and maintained to manage all property provided as GFE, purchased, or otherwise acquired for use in supporting the mission of PM MC and PEO C3T programs.

8.0. SECURITY REQUIREMENTS

The security requirements are defined in the attached DD Form 254.

a. The prime contractor is required to have a Top Secret Facility clearance, and all subcontractors are required to have a Secret Facility clearance. The prime contractor's Top Secret Facility clearance must be in place at time of proposal, and during all performance periods. The prime contractor Facility Security Officer (FSO) shall also have a Top Secret Clearance. Subcontractors may obtain their Secret Facility clearance after award. All contractor personnel shall have a minimum of a Secret Security clearance, or a Limit Access Approval (LAA) in the case of a foreign national; interim Secret Security clearances are acceptable until fully granted. All personnel located at Fort Carson, Colorado are required to have a Top Secret/Single Scope Background Investigation (TS/SSBI) clearance upon task order award. Personnel at Aberdeen Proving Ground (APG) must have a Top Secret/Sensitive Compartmented Information (TS/SCI) clearance upon task order award. These positions are defined in **ATTACHMENT A.2**. Personnel will not be permitted to perform without the required clearances.

b. The Security requirements for the task order are defined by the Department of Defense (DoD) Contract Security Classification Guide (SCG) Named "Secret Internet Protocol Routing Network (SIPRNET)" dated: 29 October 2009. The contractor will require access to COMSEC information, non-SCI intelligence information, NATO information, foreign government information and FOUO information. The contractor will require access NIPRNET, JWICS, GCCS, DMS, CENTRIX, SIPRNET at Government facilities only.

c. In performing this task order, the contractor will receive and generate classified material. Contractor will have access to classified information overseas. A COMSEC account will be required and there will be a TEMPEST requirement. Additional OPSEC requirements to the NISPOM are in effect. Use of the Defense Courier Service is authorized. Contractor personnel performing IT sensitive duties are subject to investigative and assignment requirements.

d. DoD Directive 8570.01, Information Assurance Training, Certification, and Work Force Management requires active duty military, DoD civilian, DoD consultants, and support contractor personnel performing work on sensitive automated information systems (AISs) to be assigned to positions which are designated at one of 3 sensitivity levels: (Advanced Individual Training (AIT)-I, AIT-II, or AIT-III. These designations equate to Critical Sensitive and Non-Critical Sensitive positions. The investigation requirement for AIT Level II is completion of a National Agency Check with Local Agency and Credit Checks (NACLC) with favorable results. The investigation requirement for AIT Level III is a completion of a National Agency Check with Written Inquires (NACI) with favorable results. All public release of information shall require authorization from the Government in writing. However, all information FOUO or higher will be cleared IAW Section 12 of the DD Form 254. All information gathered by the contractor to provide services to the US Government shall be considered contractually sensitive unclassified government information and shall not be released to any person or organization not part of the US Government, and shall become the property of the US Government. Information gathered, developed, analyzed, and produced under this contract remains the property of the US Army and shall be protected from unauthorized or inadvertent modification, disclosure, destruction, or use. All documentation, models, software, reports, databases and similar materials prepared under the Task Order shall be property of the U.S. submitted to PM MC at time of contract closeout in a format mutually acceptable to the Government and the contractor.

e. The contractor shall provide personnel with U.S. Security clearances as required for mission execution upon contract award. Prior to the arrival of any contractor employee to commence work under this contract at any Government site, the contractor must provide advance notice to the Government for visitor control purposes and verification of security clearance. When required, the contractor shall be tasked to access a Sensitive unclassified network, and the duties to be performed by contractor personnel under the PWS have been designated as IT-I/IT-II sensitive positions

8.1 ANTI-TERRORISM/OPERATIONS SECURITY:

1. **AT Level I training.** *This standard language is for contractor employees with an area of performance within an Army controlled installation, facility or area:*

All contractor employees, to include subcontractor employees, requiring access Army installations, facilities and controlled access areas shall complete AT Level I awareness training within XX calendar days after contract start date or effective date of incorporation of this requirement into the contract, whichever is applicable. The contractor shall submit certificates of completion for each affected contractor employee and subcontractor employee, to the COR or to the contracting officer, if a COR is not assigned, within XX calendar days after completion of training by all employees and subcontractor personnel. AT level I awareness training is available at the following website: https://Jkodirect.jten.mil/ for CAC holders. Non-CAC-holders may go to: http://jko.jten.mil/courses/atl1/launch.html.

2. **AT Awareness Training for Contractor Personnel Traveling Overseas:**

US based contractor employees and associated sub-contractor employees shall receive government provided area of responsibility (AOR) specific AT awareness training as directed by AR 525-13. Specific

AOR training content is directed by the combatant commander with the unit ATO being the local point of contact. US based contractor employees and associated sub-contractor employees will submit an Isolated Personnel Report (ISOPREP) prior to deployment, in accordance with AR 525-28, Personnel Recovery. The contractor is required to fill out the survey on NIPRNET at https://prmsglobal.prms.af.mil/prmsconv/Profile/Survey/start.aspx prior to deployment.

3. **iWATCH Training.** *This standard language is for contractor employees with an area of performance within an Army controlled installation, facility or area:*

   The contractor and all associated sub-contractors shall brief all employees on the local iWATCH program (training standards provided by the requiring activity ATO). This local developed training will be used to inform employees of the types of behavior to watch for and instruct employees to report suspicious activity to the COR. This training shall be completed within 90 calendar days of contract award and within 90 calendar days of new employees commencing performance with the results reported to the COR NLT 120 calendar days after contract award.

4. **For contracts that require a formal OPSEC program:**

   The contractor shall develop an OPSEC Standing Operating Procedure (SOP)/Plan within 90 calendar days of contract award, to be reviewed and approved by the responsible Government OPSEC officer. This plan will include a process to identify critical information, where it is located, who is responsible for it, how to protect it and why it needs to be protected. The contractor shall implement OPSEC measures as ordered by the commander. In addition, the contractor shall have an identified certified Level II OPSEC coordinator per AR 530-1.

5. **For contracts that require OPSEC Training**:

   Per AR 530-1 Operations Security, the contractor employees must complete Level I OPSEC Awareness training. New employees must be trained within 30 calendar days of their reporting for duty and annually thereafter. Level I OPSEC training is available at the following website: http://cdse.edu/catalog/elearning/GS130.html (Duration: 45 minutes).

6. **Army Training Certification Tracking System (ATCTS) registration for contractor employees who require access to government information systems:**

   All contractor employees with access to a government info system must be registered in the ATCTS (Army Training Certification Tracking System) at commencement of services, and must successfully complete the DOD Cybersecurity Awareness prior to access to the IS and then annually thereafter.

7. **For cybersecurity/information technology (IT) training:**

   All contractor employees and associated sub-contractor employees must complete the DoD Cybersecurity awareness training before issuance of network access and annually thereafter. All contractor employees working Cybersecurity/IT functions must comply with DoD and Army training requirements in DoD 8140.01, DoD 8570.01-M (Ch4) and AR 25-2 at the time of award.

8. **For cybersecurity/information technology (IT) certification**:

   Per DoD 8570.01-M (Ch4) , DFARS 252.239.7001 and AR 25-2, the contractor employees supporting Cybersecurity/IT functions shall be appropriately certified upon contract award and for any positions which are filled on a post-award basis, such contractor employees shall be certified prior to the start of performance. The baseline certification as stipulated in DoD 8570.01-M (Ch4) shall be completed upon contract award.

9. **Access and general protection/security policy and procedures.** *This standard language is for contractor employees with an area of performance within Army controlled installation, facility, or area:*

   Contractor and all associated sub-contractors employees shall provide all information required for background checks to meet installation access requirements to be accomplished by installation Provost Marshal Office, Director of Emergency Services or Security Office. Contractor workforce must comply with all personal identity verification requirements (FAR clause 52.204-9, Personal Identity Verification of Contractor Personnel) as directed by DOD, HQDA and/or local policy. In addition to the changes otherwise authorized by the changes clause of this contract, should the Force Protection Condition (FPCON) at any individual facility or installation change, the Government may require changes in contractor security matters or processes.

10. **For contracts that require handling or access to classified information.**

    Contractor shall comply with FAR 52.204-2, Security Requirements. This clause involves access to information classified “Confidential,” “Secret,” or “Top Secret” and requires contractors to comply with— (1) The Security Agreement (DD Form 441), including the National Industrial Security Program Operating Manual (DoD 5220.22-M); (2) any revisions to DOD 5220.22-M, notice of which has been furnished to the contractor.

11. **Threat Awareness Reporting Program**. *For all contractors with security clearances.*

    Per AR 381-12 Threat Awareness and Reporting Program (TARP), contractor employees must receive annual TARP training by a CI agent or other trainer as specified in 2-4b.

12. **For contractors requiring Common Access Card (CAC):**

    Before CAC issuance, the contractor employee requires, at a minimum, a favorably adjudicated National Agency Check with Inquiries (NACI) or an equivalent or higher investigation in accordance with Army Directive 2014-05. The contractor employee will be issued a CAC only if duties involve one of the following: (1) Both physical access to a DoD facility and access, via logon, to DoD networks on-site or remotely; (2) Remote access, via logon, to a DoD network using DoD-approved remote access procedures; or (3) Physical access to multiple DoD facilities or multiple non-DoD federally controlled facilities on behalf of the DoD on a recurring basis for a period of 6 months or more. At the discretion of the sponsoring activity, an initial CAC may be issued based on a favorable review of the FBI fingerprint check and a successfully scheduled NACI at the Office of Personnel Management.

13. For contractors that do not require CAC, but require access to a DoD facility or installation:

Contractor and all associated sub-contractors employees shall comply with adjudication standards and procedures using the National Crime Information Center Interstate Identification Index (NCIC-III) and Terrorist Screening Database (TSDB) (Army Directive 2014-05/AR 190-13), applicable installation, facility and area commander installation/facility access and local security policies and procedures (provided by government representative), or, at OCONUS locations, in accordance with status of forces agreements and other theater regulations.

14. For contractors authorized to accompany the force: N/A

15. Assessment and Authorization (A&A)

The Contractor shall properly implement and comply with the DoD security controls identified by the system's security plan that is approved in accordance with the process outlined in DoD 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), using the Committee on National Security Systems Instruction 1253, "Security Categorization and Control Selection for National Security Systems," and as detailed in NIST 800-53, Recommended Security Controls for Federal Information Systems in a manner consistent with the relevant Department of defense (DoD) Security Technical Implementation Guides (STIGs) to ensure that the Software will be or has been developed using secure coding and configuration practices so as to minimize security flaws within the Software and minimize misconfiguration of Commercial-off-the-Shelf (COTS) and Government-off-the Shelf (GOTS) components. Prior to the execution of a software development Work Request the Contractor shall provide the Army a copy of the Contractor's secure coding best practices policy, configuration management policy, and proactive security patching regimen policy for all COTS and GOTS components, and upon delivery of the software and system to the Army, the Contractor shall certify to the Army in writing that the Contractor complied with DoD, Army, and system level policy in the performance of its obligations to provide a compliant and secure product under the task order.

The Contractor shall update the Assessment and Authorization (A&A) documentation to ensure that the Risk Management Framework (RMF) artifacts are kept current in the Enterprise Mission Assurance Service (eMASS) and that system artifacts are properly linked to the correct controls and contain all information and supporting evidence required by the Authorizing Officer (AO) or the AO's Designated Representative. This shall include reviewing changes made to the system in order to identify any new data types that may have a Privacy Impact or change the Security Categorization of the system.

Contractor personnel performing IT Position Category duties as defined in AR 25-2 and applicable to unclassified DoD information systems, must meet the investigative and assignment requirements IAW AR 25-2 and AR 380-67. An IT Position Category Designator indicates the level of IT access required to execute the responsibilities of the position based on the potential for an individual assigned to the position to adversely impact DoD missions or functions. Position categories include: IT-I (Privileged), IT-II (Limited Privileged) and IT-III (Non-Privileged). Investigative requirements for each category are defined in Paragraph 4-14a, AR 25-2 (Reference 2). IT Position Management is the responsibility of the contractor. System Administrators (as well as Systems Engineers and Applications Administrators who may also perform System Administrator functions) are defined as IT Level I or II personnel. Upon assignment to a position, the appropriate investigation will be initiated by AR 25-2 para 4-14. If the appropriate investigative requirements cannot be favorably adjudicated, the individual will not be assigned to the IT-sensitive position. All personnel authorized privileged-level access to Information Systems (IS) are required to be trained and certified in accordance with DoD and Army policies to perform the tasks associated with their IA responsibilities based on demonstrated need-to-know and duty positions. Personnel will be required to sign a Privileged-Level Access Agreement Acceptable Use Policy and Non-Disclosure Agreement when assigned to IT-I and II positions, IAW AR 25-2. Revocation or loss of security clearance will result in immediate termination of logical and physical access to MC systems.

Classified information / material shall be protected IAW the Department of Defense, 5220.22-M, National Industrial Security Program - Operating Manual (NISPOM). Any foreign participation shall be handled IAW AR 380-10, Technology Transfer, Disclosure of Information and Contacts with Foreign Representatives, CECOM Regulation 380-16, Industrial Security, and affiliated regulations and/or supplements.

The contractor shall ensure that personnel accessing information systems have the proper and current information assurance certification to perform information assurance functions in accordance with DoD 8570.01-M, Information Assurance Workforce Improvement Program (http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf) and Army Regulation 25-2, Information Assurance. The contractor shall meet the applicable information assurance certification requirements, including:

- DoD- approved information assurance workforce certifications appropriate for each category and level as listed in the current version of DoD 8570.01-M; and
- Appropriate operating system certification for information assurance technical positions IAW DoD 8570.01-M.

Contractor personnel who do not have proper and current certifications shall be denied access to DoD information systems for the purpose of performing information assurance functions.

The contractor is responsible for background investigations.

The contractor will provide the training to meet DoD requirements for Network Enterprise Center (NEC) controlled network access as (i.e., A+; Security +; Network +).

9.0 CONTRACTOR MANPOWER REPORTING

The requirements in this PWS shall be addressed in the Army Contractor Manpower Reporting System.

The Office of the Assistant Secretary of the Army (Manpower & Reserve Affairs) operates and maintains a secure Army data collection site where the contractor will report all contractor manpower (including subcontractor manpower) required for performance of this contract. The contractor is required to completely fill in all the information in the format using the following web address: https://www.ecmra.mil/Default.aspx. The required information includes:

a. Contracting Number
b. Fiscal Year (FY that the work was performed)
c. Order Number (Delivery Order, Task Order, or Purchase Order Number)
d. Requiring Activity Unit Identification Code
e. Command (Command of the Requiring Activity that would be performing the mission if not for the contractor)
f. Contractor Name
g. Total Invoiced Amount (the total dollars amount invoiced during the fiscal year, at the deliver Order and/or Task Order Level. This is the responsibility of the Contractor)
h. Questions about Contract Performance (Contractors: Indicate if the contract/order includes the above services)
i. Government Supervision (Are the contractor personnel subject to relatively continuous supervision and control by a Government employee or officer)
j. Government's Tools and Equipment (Does the Government furnish the principal tools and equipment needed for contract performance)
k. Government Facility (Are some or all of the contractor employees provided with a workspace in a Government facility for use on a regular basis)
l. Contracting Officer (First Name, Last Name, Phone Number, and Email)
m. COR/COTR (First Name, Last Name, Phone Number, and Email)
n. Contractor (First Name, Last Name, Phone Number, and Email)
o. Location Information (Federal Supply Code (FSC), City of Installation or Services, State, Zip and Country)
p. Direct Labor Hours
q. Direct Labor Dollars
r. Fund Cite

As part of its submission, the Contractor shall provide the estimated total cost (if any) incurred to comply with this reporting requirement. The Reporting period will be the period of performance not to exceed 12 Months ending 30 September of each Government fiscal year and must be reported by 31 October of each calendar year. Contractor may use a direct XML data transfer to the database server or fill in the fields on the website. The SML direct transfer is a format for the transferring files from a contract's system to the secure web without the need for separate data entries for each required data element at the web site. The specific formats for the XML direct transfer maybe downloaded from the web.

10.0 INVOICING AND BILLING

The Contractor shall submit requests for payments in accordance with requirements below and shall provide invoice backup data as itemized below.

The Period of Performance (POP) for each invoice *shall* be for one calendar month. The Contractor shall submit only one invoice per month. The Contractor shall submit the invoice to GSA by the fifteenth (15th) calendar day of the month after the end of the invoiced month for services rendered and end of the month in which ODCs were delivered and accepted by the Government.

Each invoice shall show, the skill level category, the hours worked per skill level, the rate per skill level and the extended amount for that invoice period. It *shall* also show the total <u>cumulative</u> hours worked (inclusive of the current invoice period) per skill level, the hourly rate per skill level, the total cost per skill level, the total travel costs incurred and invoiced, and the total of any other costs incurred and invoiced, *as well as* the grand total of all costs incurred and invoiced.

Each invoice *shall clearly indicate* both the current invoice's monthly "burn rate" and the total average monthly "burn rate."

The Contractor shall submit all required documentation (unless exempted by the contract or order) as follows:

<u>Note</u>: The Government reserves the right to audit; thus, the Contractor shall keep on file all backup support documentation for travel and ODCs.

<u>Charges</u>:

- All invoice charges must be task item specific (only one task item) unless concurrent task item periods of performance exist.
- For invoices with concurrent task item periods of performance all invoice charges must be service month specific (that is one service month only).

<u>Credits:</u>

- If the credit invoice is for the same year of a particular ACT#, the contractor shall include that credit on a subsequent invoice submission against that same ACT#. If the contractor is unwilling to offset a subsequent invoice then they must submit a refund check.
- When the credit invoice is for a different year, the contractor shall submit a refund check for that credit invoice.

Invoices that net to a credit balance **SHALL NOT** be accepted. Instead a refund check must be submitted by the contractor to GSA accordingly. The refund check shall cite the ACT Number and the period to which the credit pertains. The contractor shall provide the credit invoice as backup documentation. Do not attach credit invoice in ITSS or on the Finance website. It must be attached to the refund check. The refund check shall be mailed to:

General Services Administration
Finance Division
P.O. Box 71365
Philadelphia, PA 19176-1365

Posting Acceptance Documents: Invoices shall be submitted monthly through GSA's electronic Web-Based Order Processing System, currently ITSS to allow the client and GSA COTR to electronically accept and certify services received by the customer representative (CR). Included with the invoice will be all back-up documentation required such as, but not limited to, travel authorizations and training authorizations (including invoices for such).

Receiving Agency's Acceptance: The client agency may accept and certify services electronically via GSA's electronic Web-Based Order Processing System, currently ITSS, by accepting the Acceptance Document generated by the Contractor. Electronic acceptance of the invoice by the designated client representative is considered concurrence and acceptance of services.

Content of Invoice: The Contractor's invoice shall be submitted monthly for work performed the prior month. The Contractor may invoice only for the hours, travel, ODC and services ordered by GSA and actually used in direct support of this task order. The invoice shall be submitted on official letterhead and shall include the following information, at a minimum:

1. GSA Task Order Number (from GSA Form 300, Block 2)
2. Paying Number: (ACT/DAC NO.) (From GSA Form 300, Block 4)
3. ITSS Order ID No.
4. Remittance Address
5. Period of Performance for Billing Period
6. Point of Contact and Phone Number
7. Invoice Amount
8. Itemized labor including: contractor name, labor category, skill level number and actual hours worked during the billing period and cumulative hours and totals for each employee
9. Travel Itemized by Individual and Trip (Submit the traveler's name, dates of travel, location of travel, and itemized dollar amounts of travel).
10. Other Direct Costs Itemized by Purchase (Submit itemized description of the ODC, quantity, unit price and total price of each ODC).
11. Training Itemized by Individual and Purpose (if applicable)
12. Total Invoice Amount, Current Billed, Cumulative Billed to Date

All cost presentations provided by the Contractor shall include general and administrative charges, material handling, fees, and overhead applied consistent with the Contractor's approved price proposal and consistent with DCAA/DCMA recommendations.

The Contractor shall provide the invoice data in an editable Microsoft Excel spreadsheet using a format reviewed and approved by the Government. The Government reserves the right to modify invoicing requirements at its discretion. The Contractor shall comply with any revised invoicing requirements at no additional cost to the Government.

Final Invoice/Close-out Procedures:

Interim close outs: The Government will close out each year of performance within 6 months of its expiration using the rates billed during that period. The contractor will be required to execute a waiver of claims to be included in a bi-lateral modification at the conclusion of the performance period.

Final Invoice: Invoices for the final performance period must be so identified and submitted within 6 months from completion. After this submission, no further charges are to be billed. A copy of the written client agency acceptance of task completion must be attached to the final invoice. If necessary, the contractor may request from GSA an extension for a final invoice that may exceed the 6-month time frame.

After the final invoice has been paid the contractor shall furnish a completed and signed Release of Claims (GSA Form 1142) to the Contracting Officer. This release of claims is due within fifteen (15) calendar days of final payment.

11.0 OTHER CLAUSES AND PROVISIONS INCORPORATED INTO THIS TASK ORDER

- **FAR 52.232-20 Limitation of Cost (APR 1984)**
- **FAR 52.232-22 Limitation of Funds (APR 1984)**
- **DFARS 252.227-7015 Technical Data – Commercial Items (FEB 2014)**
- **DFARS Clause 252.225-7043 - ANTITERRORISM/FORCE PROTECTION POLICY FOR DEFENSE CONTRACTORS OUTSIDE THE UNITED STATES (JUN 2015)**
- **DFARs Clause 252.232-7007 - Limitation of Government's Obligation**

- **Acceptable Skill Level Variation in Severable Labor Hour and Time and Material Orders/Contracts (July 2005)**

The Contractor may exceed the total number of labor hours per awarded skill level per base or option period, to a limit of 15% as long as the total task order obligated dollar amount per that base or option period is not exceeded, and as long as the contractor maintains an acceptable level of effort throughout the required period of performance. The contractor is not authorized to add

new skill level categories or vary between levels within the same labor category without approval of the Government, formalized in a signed modification by the contracting officer.

- **FAR 52.217-8 Option to Extend Services (NOV 1999)**

  The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 30 days of the end of the task order period of performance.

- **FAR 52.217-9 Option to Extend the Term of the Contract (Mar 2000)**

(a) The Government may extend the term of this contract by written notice to the Contractor within 30 days; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 days before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 60 months.

- **FAR 52.237-3 Continuity of Services (JAN 1991)**

(a) The Contractor recognizes that the services under this contract are vital to the Government and must be continued without interruption and that, upon contract expiration, a successor, either the Government or another contractor, may continue them. The Contractor agrees to—

(1) Furnish phase-in training; and

(2) Exercise its best efforts and cooperation to effect an orderly and efficient transition to a successor.

(b) The Contractor shall, upon the Contracting Officer's written notice, (1) furnish phase-in, phase-out services for up to 90 days after this contract expires and (2) negotiate in good faith a plan with a successor to determine the nature and extent of phase-in, phase-out services required. The plan shall specify a training program and a date for transferring responsibilities for each division of work described in the plan, and shall be subject to the Contracting Officer's approval. The Contractor shall provide sufficient experienced personnel during the phase-in, phase-out period to ensure that the services called for by this contract are maintained at the required level of proficiency.

(c) The Contractor shall allow as many personnel as practicable to remain on the job to help the successor maintain the continuity and consistency of the services required by this contract. The Contractor also shall disclose necessary personnel records and allow the successor to conduct on-site interviews with these employees. If selected employees are agreeable to the change, the Contractor shall release them at a mutually agreeable date and negotiate transfer of their earned fringe benefits to the successor.

(d) The Contractor shall be reimbursed for all reasonable phase-in, phase-out costs (i.e., costs incurred within the agreed period after contract expiration that result from phase-in, phase-out operations) and a fee (profit) not to exceed a pro rata portion of the fee (profit) under this contract.

12.0 PWS ATTACHMENTS

- ATTACHMENT A.1: Sites, Functions, Skill, & Support Staff Requirement Table
- ATTACHMENT A.2: Top Secret and Key Personnel Positions

- ATTACHMENT B: Government Furnished Equipment Status Report, To Be Issued Upon TO Award

- ATTACHMENT C: DD Form 254 Contract Security Classification Specification, Draft To Be Issued with Request For Proposal

ATTACHMENT A.1: Sites, Functions, Skill & Support Staff Requirement Table

Note: Position Descriptions are provided for guidance only and are based upon historical staffing. Contractors should propose staffing as they deem necessary to fulfill PWS requirements.

PWS Sections	Position Description	APG, MD	Ft. Carson, CO	Totals
Operations Management Support (PWS 3.1)	Helpdesk Specialist (Senior)	3	3	6
	Subject Matter Expert (Senior)	1		1
	Subject Matter Expert (Senior)	1		1
	Project Manager	1		1
	Subject Matter Expert (Journeyman)	1		1
	Technical Writer	0.8		0.8
	Technical Writer	0.8		0.8
	Technical Writer	0.1		0.1
	Business Systems Analyst	0.1		0.1
Applications Management Support (PWS 3.2)	Systems Engineer	6		6
	Systems Engineer	6		6
	Data Architect	2		2
Help Desk Support (PWS 3.3)	Helpdesk Specialist (Senior)	1	13	14
	Helpdesk Specialist (Journeyman)	1	1	2
	Information Specialist/Knowledge Engineer	5		5
	Systems Engineer	3		3
	Systems Engineer	3		3
	Systems Engineer	1		1
	Network Specialist		1	1
Engineering Support (PWS 3.4)	Helpdesk Specialist (Journeyman)	3		3
	Helpdesk Specialist (Journeyman)	3	1	4
	Information Specialist/Knowledge Engineer	1		1
Satellite Network Operations Support (PWS 3.5)	Network Specialist (Senior)	1		1
	Network Specialist (Senior)	6	2	8

IP Network Operations Support/Enterprise Architecture Support (PWS 3.6)	Network Specialist (Senior)	1		1
	Network Specialist (Senior)	0.1		0.1
Security Engineering Support (PWS 3.7)	Chief Information Security Officer	1		1
	Information Assurance/Security Specialist (Entry Level)	1		1
Test Event and Training Support (PWS 3.8)	Network Specialist (Journeyman)	2		2
Software Development Support (PWS 3.9)	Subject Matter Expert (Senior)	10		10
Grand Total		**65.9**	**21**	**86.9**

ATTACHMENT A.2: Top Secret and Key Personnel Positions

TOP SECRET AND KEY PERSONNEL						
		TS/SCI	TS/SSBI	KEY	KEY	KEY
PWS Sections	**Position Description**	**APG, MD**	**Ft. Carson, CO**	**APG, MD**	**Ft. Carson, CO**	**TOTAL**
Operations Management Support (PWS 3.1)	Helpdesk Specialist (Senior)		3			
	Subject Matter Expert (Senior)	1		1		1
	Subject Matter Expert (Senior)	1		1		1
	Project Manager			1		1
Applications Management Support (PWS 3.2)	Systems Engineer					
	Systems Engineer					
Help Desk Support (PWS 3.3)	Helpdesk Specialist (Senior)		13			
	Helpdesk Specialist (Journeyman)		1			
	Network Specialist (Journeyman)		1	5	1	6
	Network Specialist				1	1
Engineering Support (PWS 3.4)	Helpdesk Specialist (Journeyman)		1			
Satellite Network Operations Support (PWS 3.5)	Network Specialist (Senior)			1		1
	Network Specialist (Senior)		2	6	2	8
Security Engineering Support (PWS 3.7)	Information Assurance/Security Specialist (Entry)			1		1
Total		2	21	16	4	20